自己双対クロンのrigidity問題 (計算機科学の基礎理論 : 21世紀の計算パラダイムを目指して)

AUTHOR(S):

宮川, 正弘; ローゼンバーグ, Ivo. G.

CITATION:

宮川, 正弘 ...[et al]. 自己双対クロンのrigidity問題 (計算機科学の基礎理論 : 21世紀の計算パラダイムを目指して). 数理解析研究所講究録 2000, 1148: 1-4

ISSUE DATE:

2000-04

URL:

http://hdl.handle.net/2433/64024

数理解析研究所講究録
1148巻 2000年 1-4

自己双対クロンの rigidity 問題

宮川正弘
(Masahiro Miyakawa)
筑波技術短期大学
mamiayaka@cs.k.tsukuba-tech.ac.jp

Ivo.G. ローゼンバーグ
(Ivo.G. Rosenberg)
Montreal 大学
rosenb@dms.umontreal.ca

Abstract

$A := \boldsymbol{k} = \{0, ..., k-1\}$, $k > 1$ の値をとる多値論理関数の閉じた関数集合族（クロン clones）において，反射的関係で記述されるクロンの共通集合が trivial 関数集合（射影関数の集合 $J = \{f(x_1, \ldots, x_n) := x_i | i = 1, \ldots, n\}$ と定数関数の集合の和集合）となる場合がある (semirigidity 問題) のと対照的に，自己双対クロン族（1 変数関数から決まる関係を保存する関数族; この関係は反射的でない）の共通部分が射影関数の集合 J となることは決してない事 (Proposion 7) を示す。あわせて，自己双対クロンの共通集合に関する (rigidity) 問題から発生する次の 2 つの問題を考察し，部分的な解を与える。

問題 1. $\boldsymbol{k}$ の上の置換の集合 R で，次の 2 条件を満たすものを求める。(1) 全ての $r \in R$ は同じ素数長さのサイクルの積である，(2) R の全ての元と可換な $\boldsymbol{k}$ の上の 1 変数関数は恒等写像 e に限る。

問題 2. 任意の 1 変数関数の集合 $R \subseteq O^{(1)}$ の元から誘起される クロン $\mathrm{Pol}\, r^{\square}$ のすべての $r \in R$ の共通部分で定まるクロン（R の endoprimal クロン）C の 1 変数関数の集合 $C^{(1)}$ が恒等写像 e のとき，$C^{(n)} \not\subseteq J$ となる最小の n を求める。

1. 背景と問題

空でない基底集合 A を固定する．正の整数 $n > 0$ に対して $O_A^{(n)}$ で A の上の全ての n 変数演算 あるいは関数 (=写像 f: $A^n \to A$) の集合をあらわし，$O_A := \bigcup_{n=1}^{\infty} O_A^{(n)}$ とする．例えば $1 \leq i \leq n$ について，n 変数の i 番目の**射影** と呼ばれる n 変数演算 e_i^n は $e_i^n(a_1, \ldots, a_n) := a_i$ for all $a_1, \ldots, a_n \in A$ で定義される．

クロン（閉じた集合）. 全ての射影関数の集合を J_A で表す。O_A の部分集合で，関数の合成に関して閉じており，J_A を含んだものはクロン *clone* と呼ばれる。(クロンの定義や一般代数 (universal algebra) における意味付けについては文献 [4] にある)。例えば，集合 J_A や O_A はクロンである。全ての定数関数（すなわち $|im\ f| = 1$ である $f \in O_A^{(n)}$ の集合）の集合を c_A で表す。射影関数と定数関数の和集合 $K_A := J_A \cup c_A$ を **trivial 関数**と呼ぶ。trivial 関数もクロンである。包含関係を順序とし，集合の共通部分を meet 演算としたとき，A の上の全てのクロンは J_A を最小元，O_A を最大元とする束 L_A をなす。有限集合 $|A| > 2$ のときこの束の様子は十分には分かっていない。しかし，この束の極大元（dual atoms, = coatomes) すなわち O_A の直下の元は **極大** *maximal* **or** *precomplete* **クロン**と呼ばれ，全て既知であり，任意のクロンはいずれかの極大元の部分クロンとなっている。

関係を保存する関数. h を正の整数とするとき，A^h の部分集合 ρ(A の元の h 組の集合）を A の上の **h 項関係**と呼ぶ。n **変数関数** $f \in O_A$ **が** ρ **を保存する**とは，各列を ρ から任意に取って作成した h 行 n 列の任意の行列 $X = [x_{ij}]$ に対して，常に

$$(f(\boldsymbol{x}_1), f(\boldsymbol{x}_2), \ldots, f(\boldsymbol{x}_h)) \in \rho$$

が成り立つことである。例えば，ρ が (部分) 順序関係 $\leq$ (すなわち反射的，反対称的，推移的 2 項関係）のとき，f が $\leq$ を保存するのは，f が単調関数，すなわち $x_{11} \leq x_{21}, \ldots, x_{1n} \leq x_{2n}$ のとき $f(\boldsymbol{x}_1) \leq f(\boldsymbol{x}_2)$ となるときである。与えられた関係 ρ を保存する関数の集合を $\mathrm{Pol}\, \rho$ で表す。

A の上の 1 変数関数 $s \in O^{(1)}$ について，関係 $s^{\square} := \{(a, s(a)) : a \in A\}$ （2 項関係）を関数 s が定める**関数的関係**と呼ぶ。s が置換（すなわち，1:1 全射関数）の場合だけでなく，一般の関数についても，関数的関係を保存する関数を**自己双対関数**と呼ぶ。関数的関係 $s^{\square}$ は，恒等写像 e を除いて，反射的でない。

semirigidity 問題と rigidity 問題. 反射的関係（$(a, a) \in r$ for every $a \in A$）を保存するクロンは定数と射影関数 (すなわち K_A) を必ず含む。よって，$\{\rho_i | i \in I\}$ を反射的関係の集合とすると，$K_A \subseteq \bigcap_{i \in I} Pol\ \rho_i$(射影と定数の和集合) が成り立つ。特に等号が成り立つとき，その反射的関係の集合 $\{\rho_i\}$ を *semirigid* と呼ぶ。関係 ρ_i として関数的関係をとると，右辺には (定数が含まれず) 全ての射影関数の集合が J_A が含まれるので K_A を J_A で置き換えた式

$$J_A \subseteq \bigcap_{i \in I} Pol\ \rho_i$$

がなりたつ。ここで特に等号が成り立てばその関数的関係の集合をを rigid と呼ぶ。問題は semirigid あるいは rigid な部分集合を決定することである。

クロン C の 1 変数関数の集合 $C^{(1)} := C \cap O^{(1)}$ を クロン C の基盤 (*foundation*) と呼ぶ。クロンの semirigidity あるいは rigidity をその基盤で判定できるであろうか。

semirigidity 問題はは次数 (arity) を 1 変数に制限して，すなわちクロンの基盤だけを考察して判定できる [3]。一方，rigidity 問題についてはこれは成り立たない [8]。後に示すように（命題 7），rigid な関数的関係の集合は存在しない。全ての関数的関係の集合 $R = \{r^{\square} : r \in O^{(1)}\}$ のなす "endoprimal" クロンは"synchronous" 関数と一致する [7]。synchronous

関数は1変数，2変数，...，k 変数関数までは射影関数 $J^{(1)},\ldots,J^{(k)}$ と一致する。従って，2つのクロンの基盤が rigid でも $k+1$ 変数までいけば，かならず本質的に2変数以上の関数を含むことになるが，クロンの2変数部分から k 変数部分までの何処でこれが起こるかはいまのところ調べられていない。他に，その endoprimal クロンが synchronous 関数と一致するような，1変数関数の集合 $R\subset O^{(1)}$ は存在するかどうかまだ考察されていない。$O^{(1)}$ の代わりに，自己双対極大クロンを与える置換の集合 S^* の部分集合 R でそのようなものが存在するかどうかもまだ考察されていない。

2. Rigidity

ここでは1変数関数の集合についてのみ問題を特化する。

$A=\boldsymbol{k}$ の上の全ての1変数関数 $O^{(1)}$ の2元 f,g について，

$$f\circ g=g\circ f$$

が成立するとき，f と g は**可換**といわれる（$h(x)=f\circ g:=f(g(x))$ for all $x\in\boldsymbol{k}$）。

$R\subset O^{(1)}$ が **rigid** とは，R の全ての元 $r\in R$ と可換な $O^{(1)}$ の元が，恒等写像 e のみに限る場合を言う。問題は，集合 $O^{(1)}$ の部分集合が rigid となる条件をもとめる事である。解は部分的にしか分っていない。ここでは，rigid であるための十分条件と，$\boldsymbol{k}$ の置換の rigid でない対 $\{r,s\}$ の大きなクラスを与える。

R の（写像）合成演算 $\circ$ に関する閉包を $\langle R\rangle$ と書けば，それは，R を含み，任意の $f,g\in\langle R\rangle$ について，$f\circ g\in\langle R\rangle$ を満たす $O^{(1)}$ の最小な集合と一致する。$f\in O^{(1)}$ が R の任意の元と可換であるならばそれは $\langle R\rangle$ の任意の元と可換である（逆は閉包の定義から自明）。

$v\in O^{(1)}$ の**不動点**の集合を

$$\mathrm{Fix}\ v:=\{a\in\boldsymbol{k}:\ v(a)=a\}.$$

で表す。また，$a\in\boldsymbol{k}$ の R-**軌跡** を $\{v(a):\ v\in\langle R\rangle\}$ で定義する。a の R-軌跡とは任意の $v\in R$ に対して $v(a)$ を含み，任意の $u\in\langle R\rangle$ を作用させても閉じている最少な $\boldsymbol{k}$ の部分集合である。

$a\in\boldsymbol{k}$ に対して

$$[a]_R:=\cap\{\mathrm{Fix}\ v:v\in\langle R\rangle,a\in\mathrm{Fix}\ v\}$$

と置く。a を不動点とする $v\in R$ がないときは，$[a]_R:=\boldsymbol{k}$ と定義する。$[a]_R$ は a を不動点として含む $r\in\langle R\rangle$ の全ての不動点 (fixed) 集合の共通部部分（平たく言えば，a の近傍にあり $\langle R\rangle$ の任意の元の不動点の集合に含まれる点の集合である）。

Proposition 1. $R\subseteq O^{(1)}$ とし，$u\in O^{(1)}$ が任意の $r\in R$ と可換とする。$a\in\boldsymbol{k}$ とする。このとき *(i)* $u(a)\in[a]_R$, *(ii)* 任意の正の整数 ℓ について $u^\ell(a)\in[a]_R$, *(iii)* $[a]_R=\{a\}$ ならば Fix u は a の R-軌跡を含む。

Corollary 2. $R\subseteq O^{(1)}$ とする。ある $A\subset\boldsymbol{k}$ があって，A の各点 a について *(1)* $[a]_R=\{a\}$ で，*(2)* a の R-軌跡の $a\in A$ に対する和集合が $\boldsymbol{k}$ となれば，R は *rigid* である。特に，*(1)* $[a]_R=\{a\}$ で，*(2)* a の R-軌跡が $\boldsymbol{k}$ となる $a\in\boldsymbol{k}$ があれば，R は *rigid* である。

rigid な集合の例をあげる。

Example 3. $k=6$ とし 次の表の $r,s\in O^2$ で定まる $R=\{r,s\}$ は *rigid* である（*3*節の終わりの記法に従えば $r,s\in S^{(3)}$）。

x	0	1	2	3	4	5
r(x)	1	0	2	4	5	3
s(x)	1	3	5	0	2	4

実際，$t:=s^2\circ r$ について，$\mathrm{Fix}(t)=\{0\}$ より，$[0]_R=\{0\}$ であり，0 の R 軌跡は**6**である。

x	0	1	2	3	4	5
$s^2(x)$	3	0	4	1	5	2
$t(x)$	0	3	4	5	2	1

rigid ではないいくつかの集合を示す。

Lemma 4. m,n を正の整数とし m を偶数とする。$i\le i'$ なる異なる対 $(i,j),(i',j')$ が次式：

$$a_{ij}=a_{i'j'}\Longleftrightarrow j'=0,i=i'-1,j=j'+1$$

を満たしている集合 $\{a_{ij}\in\boldsymbol{k}:\ 0\le i<m,0\le j<n\}$ を考える（以下，最初の添字は mod$m$ で *2*番目の添字は mod$n$ でとる*)*.

$$A:=\boldsymbol{k}\setminus\{a_{ij}:0\le i<m,0\le j<n\}.$$

と置く。$r\in O^{(1)}$ が

$$r(a_{ij})=\begin{cases}a_{i,j+1} & \text{if } i \text{ is even},\\ a_{ij} & \text{if } i \text{ is odd},\ 0<j<n\end{cases}$$

および $r(A)\subseteq A$ を満たすとする。同様に，$s\in O^{(1)}$ が

$$s(a_{ij})=\begin{cases}a_{i,j+1} & \text{if } i \text{ is odd},\\ a_{ij} & \text{if } i \text{ is even},\ 0<j<n\end{cases}$$

および $s(A)\subseteq A$ をみたすとする。このとき，$\{r,s\}$ は *rigid* ではない。

Remark. r と s が 集合 $\boldsymbol{k}\setminus A$ の置換になっていることは明らかである．$n=2$ のとき r を $\boldsymbol{k}\setminus A$ に制限した関数は，i を偶数とした 2-サイクル (a_{i0},a_{i1}) で，また s は，i を奇数とした 2-サイクル (a_{i0},a_{i1}) となっている．($m=4,n=2$ を Fig. 1 に，$m=4,n=3$ を Fig.2 に示す。太い線は，r による遷移を，また細い線は s による遷移を示す。)

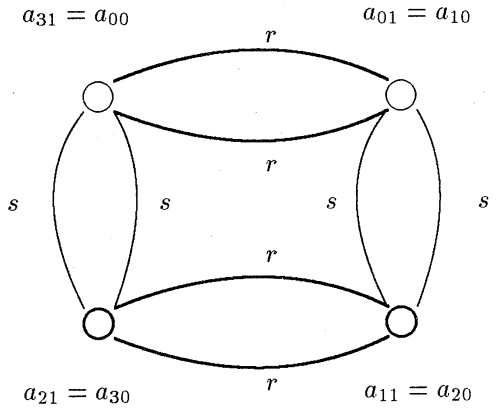

Figure 1: Transition diagram (a)

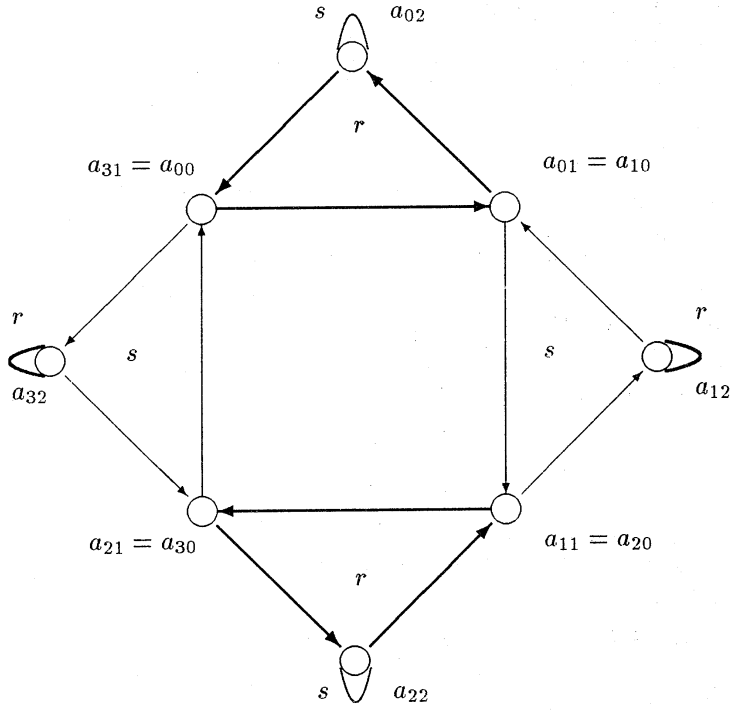

Figure 2: Transition diagram (b)

Corollary 5. 正の整数 m と互いに異なる $a_{2i,j} : i = 0, \ldots, m,\ j = 0, 1$ が $\boldsymbol{k}$ にあり，全ての $i = 0, \ldots, m$ について，r, s が

$$\begin{array}{llll} r(a_{2i,0}) & := a_{2i,1}, & r(a_{2i,1}) & := a_{2i,0}, \\ s(a_{2i,0}) & := a_{2(i-1),1}, & s(a_{2(i-1),1}) & := a_{2i,0}\,. \end{array}$$

を満たすものとする。このとき，$\{r, s\}$ は *rigid* ではない。

Theorem 6. k が偶数のとき，長さが 2 のサイクルの積からなる任意の 2 つの置換 s と t は *rigid* ではない。

3. 自己双対クロンの共通集合

$s \in O^{(1)}$ について，関数 $f \in O^{(n)}$ が関係

$$s^{\square} := \{(x, s(x)) : x \in \boldsymbol{k}\}$$

を保存するのは 全ての $a_1, \ldots, a_n \in \boldsymbol{k}$ について

$$f(s(a_1), \ldots, s(a_n)) = s(f(a_1, \ldots, a_n)),$$

が成り立つときである。任意の $R \subseteq O^{(1)}$ についてその共通部分のなすクロン

$$C := \cap\{\mathrm{Pol}\, r^{\square} : r \in R\}$$

を R の **endoprimal** クロンと呼ぶ。関係の理論を用いて証明される次の命題は，任意の endoprimal クロンが必ず 2 個以上の本質変数を含む，すなわち任意の endoprimal クロンは射影関数 J よりも必ず大きい事を意味している。

Proposition 7. 任意の $R \subseteq O^{(1)}$ について $C := \cap\{\mathrm{Pol}\, r^{\square} : r \in R\}$ は必ず J と異なる。

実際，Proposition 7 において $R = O^{(1)}$ とした特別な（右辺が最小となる）場合を町田 [7] は考察し，最小の endoprimal クロンが，“synchronous” と名づけた関数の集合と一致する事を示した。

Theorem 8. $R = O^{(1)}$ と置く。R の *endoprimal* クロンは次に定義する *synchronous* 関数の集合と一致する。すなわち，

$$C_R := \{\cap \mathrm{Pol}\, s^{\square} | s \in R\} = \{\text{synchronous 関数}\}.$$

いま，$n > k$ とする。$f^{(n)}$ の引数ベクトル $\boldsymbol{a} = (a_1, \ldots, a_n) : \cup_{i=1}^{n}\{a_i\} = \boldsymbol{k}$ をその値により k 分割し図式的に，$\boldsymbol{a} = (0, \ldots, 0, \ldots, k-1, \ldots, k-1)$ と書く。ベクトル $\boldsymbol{a}$ と $\boldsymbol{b}$ が関係している (related) のは，ある $\varphi \in O^{(1)}$ があって，$\boldsymbol{b} = \varphi(\boldsymbol{a})$，すなわち $b_i = \varphi(a_i),\ 1 \le i \le n$ と書けるときである。

$f \in O^{(n)}$ が **synchronous** 関数と呼ばれるのは次が成り立つ場合である。

引数 $\{1, 2, \ldots, n\}$ の任意の k-分割 $\{A_0, \ldots, A_{k-1}\}$ (すなわち，$\cup_{i=0}^{k-1} A_i = \{1, \ldots, n\}$, $A_i \cap A_j = \emptyset$ for every $i \neq j$) について，以下のことがらが成り立つ：

（任意の）ある写像 $\varphi : \boldsymbol{k} \to \boldsymbol{k}$ （すなわち，$\varphi \in O^{(1)}$）にたいして，

$$f(\varphi(0), \ldots, \varphi(0), \ldots, \varphi(k-1), \ldots, \varphi(k-1)) = \varphi(j) \quad (1)$$

$(0 \leq j \leq k)$ が成立していれば，任意の写像 $\psi : \boldsymbol{k} \to \boldsymbol{k}$ に対して，

$$f(\psi(0), \ldots, \psi(0), \ldots, \psi(k-1), \ldots, \psi(k-1)) = \psi(j). \tag{2}$$

が成り立つ。

明らかに synchronous 関数は n 個の変数に依存する。また，上の定義から，synchronous 関数は任意の自己双対関数に含まれる事が用意に導かれる。関数的関係に対する最小の endopprimal クロン である synchronous 関数 は $n = k$ 変数までは，射影関数 $e = J^{(1)}, J^{(2)}, \ldots, J^{(k)}$ しか含んでいない。次で定義される discriminator 関数 [11]

$$t(x, y, z) = \begin{cases} z & \text{if } x \neq y \\ x & \text{otherwise} \end{cases} \tag{3}$$

は synchronous 関数の例である。Boole 関数 $(k = 2)$ についても，3 変数以上では synchronous 関数は存在する。

自己双対クロンの基盤については，次が成り立つ [8]。

Proposition 9. *k が素数のとき，任意の 2 つの自己双対極大クロンの基盤は rigid である。*

これより，

Corollary 10. *k 素数のとき，任意の 2 つの異なる自己双対極大クロンを与える置換 r, s （すなわち $r, s \in S^*$）に対して，次が成り立つ： $n > k$ のとき*

$$\begin{aligned} \mathrm{Pol}\, r^{\square})^{(1)} \cap \mathrm{Pol}\, s^{\square})^{(1)} &= \{e\} \\ \mathrm{Pol}\, r^{\square})^{(n)} \cap \mathrm{Pol}\, s^{\square})^{(n)} &\supseteq \{n\text{-変数 } \textit{synchronous} \text{ 関数 }\}. \end{aligned}$$

以上の事実は，反射的関係については成立した 1 変数帰着がいつでも成り立たない事を示している。

S_k を $A := \boldsymbol{k} := \{0, \ldots, k-1\}$ の上の全ての置換の集合（対称群）とする。n が k を割るとき，不動点を持たない置換 $f \in S_k$ で，その全てのサイクルが長さ n である全ての置換の集合を $S^{(n)}$ で表す。

$$S^* := \cup\{S^{(p)} : p \text{ prime divisor of } k\}$$

とする。

$s \in S_k$ のとき，$\mathrm{Pol}\, s^{\square}$ は置換 s についての**自己双対関数**となる。$\mathrm{Pol}\, s^{\square}$ が極大クロンとなるのは $s \in S^*$ となるときであり，そのときに限る。極大自己双対クロンの基盤の rididity 問題は k 素数のときを除いて一般的には未解決である（2 章で考察した問題の部分問題）。また，自己双対極大クロンの集合から生成する endoprimal クロンの次のような問題についても調べられていない。

$s_1, \ldots, s_m \in S^*$ について

$$(\cap_{i=1}^{m} \mathrm{Pol}\, s_i^{\square})^{(1)} = \{e\} \quad \text{（恒等写像）}$$

が成り立つときある arity n で初めて

$$\cap_{i=1}^{m} (\mathrm{Pol}\, s_i^{\square})^{(n)} \supset J^{(n)} \quad \text{（射影関数）}$$

が成り立つような n を求める（定理 8 からこのような n は $1, n \leq k$ の範囲にあることがわかる）。

謝辞. 命題 7 の別解をご指摘いただいき，討論していただいた町田 元氏（一ツ橋大学）に感謝いたします。

References

[1] V.G.Bondarchuk, L.A.Kaluzhnin, V.N.Kotov, A.A.Romov, The Galoia theory for Post algebras I-II (Russian), *Kibernetika* (Kiev) **3** (1969), 1-10; **5** (1969), 1-9; English tranaslation: *Systems Theory Resaearch* **3**.

[2] Demetrovics J., Miyakawa, M., Rosenberg I.G., Simovici D., Stojmenović I., Intersections of isotone clones on a finite set, *Proc. 20th International Symp. on Multiple-Valued Logic,* Charlotte, 1990, 248-253.

[3] Länger, F., Pöschel R., Relational systems with trivial endomorphisms and polymorphisms. J. Pure Appl. Algebra **32** (1984) 2, 129-142.

[4] Lau, D., Funktionenalgebren über endlichen Mengen Band 1, Monograph, Universität Rostock, pp. 592.

[5] Laskia, V., Miyakawa, M., Nozaki, A., Pogosyan, G., Rosenberg, I.G., Semirigid sets of diamond orders, Discrete Mathematics 156(1996), 277-283.

[6] Miyakawa M.,Nozaki A.,Pogosyan G., Rosenberg I.G., Semirigid sets of central relations over a finite domain, *Proc. 22th International Symposium on Multiple-Valued Logic*, Sendai, May 27-29, 1992, 300-307.

[7] 町田元，“Synchronous 関数族について”, 2000.

[8] Miyakawa M, Semirigidity problems in k-valued logic, *Proc. 29th International Symp. on Multiple-Valued Logic*, Freiburg, 1999, 256-260; 多値論理代数における semirigidity 問題，数解研講究録 1093, 1-4, 1999.

[9] Nozaki A., Miyakawa M., Pogosyan G. and Rosenberg I.G., The number of orthogonal permutations, Europ. J. Combinatorics (1995) **16**, 71-85.

[10] Nozaki A., Pogosyan G., Miyakawa M. and Rosenberg I.G., Semirigid sets of quasi-linear clones, *Proc. 23rd International Symp. on Multiple-Valued Logic*, Sacramento, 1993, 105-110.

[11] Pixley A.F., Functionally complete algebras generating distributive and permutable classes, Math. Z. **114**,361-372, 1970.

[12] Pöschel R., Kalužnin L.A., *Funktionen und Relationen Algebren*, Ein Kapitel der Diskreten Mathematik (German), Math. Monographien B. 15, VEB Deutscher Verlag d. Wissen., Berlin, 1979, 259 pp. Also Math. R. B. 67, Birkhäuser Verlag, Basel & Stuttgart, 1979.